QUANTUM COMPUTATION - FALL 2006 - EXERCISE 2

Due: 11/12/06. Submission in pairs, to Elad's mailbox in Ross.

1. Universal Reversible Computation

1.1. Show that the Toffoli gate is a universal gate with respect to reversible classical computation.

1.2. Show that there is no set of 2 bit gates which is universal with respect to reversible classical computation.

2. Teleportation

Suppose Alice and Bob share two pairs of EPR states, and they wish to apply Teleportation of a state of two qubits instead of one. The two qubits may be in an arbitrary (possibly entangled) quantum state. Write a quantum circuit that does the trick, and prove that it works for any initial state of two qubits.

3. Order Of Application Of Gates Within A Circuit

A quantum circuit is a directed graph, which contains no cycles, and in which each node represents a unitary gate from some universal set of unitary gates. It has inputs (some of which may be constant states) and outputs (i.e., marked qubits to be measured at the end.)

Show that the order in which the gates are operated on the input state of the circuit does not affect the final output state of the circuit, as long as this order corresponds to a topological order of the nodes in the graph.

4. Locality of measurements

4.1. Let $|\alpha\rangle$ be an arbitrary state in a Hilbert space of dimension n, and let $V = \{|v_1\rangle, \dots, |v_n\rangle\}$ be an orthonormal basis to that space. Show that there exists a unitary matrix U, such that measuring $|\alpha\rangle$ in the basis V is equivalent to measuring $|U\alpha\rangle$ in the *standard* basis.

4.2. Consider a bipartite quantum state $|\psi\rangle_{A,B}$. Show that if Alice performs an measurement in an arbitrary basis on her part of the system, and then Bob measures his qubits in the standard basis, then Bob's measurement outcome is independent of Alice's actions.

Conclude that there is no measurement that Bob can perform to tell which measurement Alice performed on her qubits.

5. Do We Really Need Complex Numbers?

Prove that we can assume w.l.o.g that all amplitudes in a quantum computation are real numbers! **Guidence:** Show that any quantum circuit on n qubits that uses t two-qubit gates can be simulated exactly by a quantum circuit on $n+1$ qubits, that uses at most t three-qubit gates. (Hint: use the extra qubit to decide whether we are in the Imaginary or Real world, and adapt each gate to a gate with one more qubit, such that the new gate works in an equivalent way to the old one.